Qcrypt tutorial:
Security analysis of practical QKD

Charles Lim

Department of Electrical & Computer Engineering, National University of Singapore
Centre for Quantum Technologies, National University of Singapore

Context and motivation

The security of practical QKD is an area of active research in the community.

Here, we focus on the **security of finite-length keys** and some of the latest results on the **security of QKD with imperfect transmitters**.

Context and motivation

The security of practical QKD is an area of active research in the community.

Here, we focus on the **security of finite-length keys** and some of the latest results on the **security of QKD with imperfect transmitters**.

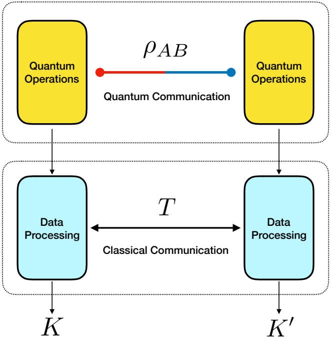
Tutorial topics:

1. Security of QKD (concepts and tools)
2. Example 1: finite-key security of BBM92
3. Numerical methods for QKD
4. General framework and recent developments
5. Example 2: MDI-QKD with security against arbitrary Trojan-horse attacks

It is the art of using quantum systems to exchange cryptographic keys between two remote parties who are connected by a pair of channels: an authenticated[1] classical channel and an insecure quantum channel.

[1] For this, we need to assume that the users have access to some initial pool of secret keys.

It is the art of using quantum systems to exchange cryptographic keys between two remote parties who are connected by a pair of channels: an authenticated[1] classical channel and an insecure quantum channel.



The protocol is a LOCC (local operations & classical comms) map:

$$\mathcal{E}^{\mathsf{QKD}}_{AB\to KK'T} : \rho_{AB} \to \rho_{KK'T},$$

where K and K' are Alice's and Bob's secret key registers and T is the register capturing all of classical information exchanged over the public channel. Moreover,

$$\rho_{AB} = \mathrm{Tr}_E(|\Psi\rangle\langle\Psi|_{ABE}).$$

[1] For this, we need to assume that the users have access to some initial pool of secret keys.

Let K and K' take values from $\mathcal{K}_\ell \cup \{\perp\}$, where $\mathcal{K}_\ell := \{0,1\}^\ell$ and $\perp$ indicates *protocol failure* (hash error, high QBER, etc).

Let K and K' take values from $\mathcal{K}_\ell \cup \{\perp\}$, where $\mathcal{K}_\ell := \{0,1\}^\ell$ and $\perp$ indicates *protocol failure* (hash error, high QBER, etc).

The output state is then given by

$$\mathcal{E}^{\text{QKD}}_{AB \to KK'T}(|\Psi\rangle\langle\Psi|_{ABE}) = \rho_{KK'TE},$$

where

$$\rho_{KK'TE} := p_\perp |\perp,\perp\rangle\langle\perp,\perp|_{KK'} \otimes \sigma_{TE} + \tau_{KK'TE}, \tag{1}$$

$p_\perp$ is the abort probability and

$$\tau_{KK'TE} := \sum_{k,k' \in \mathcal{K}_\ell} P_{KK'}(k,k') \big|k,k'\big\rangle\big\langle k,k'\big|_{KK'} \otimes \underbrace{\tau^{k,k'}_{TE}}_{\text{Eve's quantum side info}} \tag{2}$$

Let K and K' take values from $\mathcal{K}_\ell \cup \{\perp\}$, where $\mathcal{K}_\ell := \{0,1\}^\ell$ and $\perp$ indicates *protocol failure* (hash error, high QBER, etc).

The output state is then given by

$$\mathcal{E}^{\mathrm{QKD}}_{AB\to KK'T}(|\Psi\rangle\langle\Psi|_{ABE}) = \rho_{KK'TE},$$

where

$$\rho_{KK'TE} := p_\perp |\perp,\perp\rangle\langle\perp,\perp|_{KK'} \otimes \sigma_{TE} + \tau_{KK'TE}, \tag{1}$$

$p_\perp$ is the abort probability and

$$\tau_{KK'TE} := \sum_{k,k'\in\mathcal{K}_\ell} P_{KK'}(k,k')\big|k,k'\big\rangle\big\langle k,k'\big|_{KK'} \otimes \underbrace{\tau^{k,k'}_{TE}}_{\text{Eve's quantum side info}} \tag{2}$$

Note that $\tau_{KK'TE}$ is sub-normalised with its trace giving the probability that the protocol succeed,

$$\mathrm{Tr}(\tau_{KK'TE}) = 1 - p_\perp. \tag{3}$$

Recall that the goal of QKD is to produce **a pair of perfectly correlated secret keys**. These conditions suggest that the ideal output state is of the form,

$$\rho^{\text{ideal}}_{KK'TE} = p_\perp |\perp,\perp\rangle\langle\perp,\perp|_{KK'} \otimes \sigma_{TE} + \underbrace{\omega_{KK'} \otimes \tau_{TE}}_{\text{product state}}, \tag{4}$$

where

$$\omega_{KK'} := \sum_{k,k' \in \mathcal{K}_\ell : k=k'} 2^{-\ell} |k,k'\rangle\langle k,k'|_{KK'}, \tag{5}$$

is a perfectly uniform state with perfectly correlated outcomes between K and K'.

Recall that the goal of QKD is to produce **a pair of perfectly correlated secret keys**. These conditions suggest that the ideal output state is of the form,

$$\rho^{\text{ideal}}_{KK'TE} = p_\perp |\perp,\perp\rangle\langle\perp,\perp|_{KK'} \otimes \sigma_{TE} + \underbrace{\omega_{KK'} \otimes \tau_{TE}}_{\text{product state}}, \tag{4}$$

where

$$\omega_{KK'} := \sum_{k,k' \in \mathcal{K}_\ell : k=k'} 2^{-\ell} |k,k'\rangle\langle k,k'|_{KK'}, \tag{5}$$

is a perfectly uniform state with perfectly correlated outcomes between K and K'. Likewise, we have that

$$\mathrm{Tr}(\omega_{KK'} \otimes \tau_{TE}) = 1 - p_\perp. \tag{6}$$

Def: Security criterion

We say that the protocol $\mathcal{E}^{\mathrm{QKD}}_{AB\to KK'T}$ is ϵ_{QKD}-*secure* if its output satisfies the so-called *trace-distance criterion*[a]:

$$\frac{1}{2}\left\|\rho_{KK'TE}-\rho^{\mathrm{ideal}}_{KK'TE}\right\|_1 \leq \epsilon_{\mathrm{QKD}}. \tag{7}$$

[a] See Portmann & Renner, arXiv:2102.00021 (2021) and references therein.

Def: Security criterion

We say that the protocol $\mathcal{E}^{\mathrm{QKD}}_{AB\to KK'T}$ is ϵ_{QKD}-*secure* if its output satisfies the so-called *trace-distance criterion*[a]:

$$\frac{1}{2}\left\|\rho_{KK'TE} - \rho^{\mathrm{ideal}}_{KK'TE}\right\|_1 \leq \epsilon_{\mathrm{QKD}}. \tag{7}$$

[a] See Portmann & Renner, arXiv:2102.00021 (2021) and references therein.

Since the protocol is by definition secure when it aborts, the criterion can be expressed as

$$\frac{1}{2}\left\|\rho_{KK'TE} - \rho^{\mathrm{ideal}}_{KK'TE}\right\|_1 \leq (1-p_\perp)\frac{1}{2}\left\|\tilde{\tau}_{KK'TE} - \omega_{KK'}\otimes\tilde{\tau}_{TE}\right\|_1, \tag{8}$$

where $\tilde{\tau}_{KK'TE}$ and $\tilde{\tau}_{TE}$ are renormalized states (with $1-p_\perp$).

Def: Security criterion

We say that the protocol $\mathcal{E}^{\text{QKD}}_{AB\to KK'T}$ is ϵ_{QKD}-*secure* if its output satisfies the so-called *trace-distance criterion*[a]:

$$\frac{1}{2}\left\|\rho_{KK'TE}-\rho^{\text{ideal}}_{KK'TE}\right\|_1 \le \epsilon_{\text{QKD}}. \tag{7}$$

[a] See Portmann & Renner, arXiv:2102.00021 (2021) and references therein.

Since the protocol is by definition secure when it aborts, the criterion can be expressed as

$$\frac{1}{2}\left\|\rho_{KK'TE}-\rho^{\text{ideal}}_{KK'TE}\right\|_1 \le (1-p_\perp)\frac{1}{2}\left\|\tilde{\tau}_{KK'TE}-\omega_{KK'}\otimes\tilde{\tau}_{TE}\right\|_1, \tag{8}$$

where $\tilde{\tau}_{KK'TE}$ and $\tilde{\tau}_{TE}$ are renormalized states (with $1-p_\perp$).

Importantly, this notion of security possesses the property of *composability*, in the sense that it preserves the security (error) of the protocol even if it is embedded into a larger crypto-system.

The central goal is to establish a tight bound on security error in terms of the protocol parameters (block size, QBER threshold, key length, etc). The security of QKD can be analyzed in two (independent) parts—*correctness* and *secrecy*.[2]

[2] See Renner PhD Thesis (2005).

The central goal is to establish a tight bound on security error in terms of the protocol parameters (block size, QBER threshold, key length, etc). The security of QKD can be analyzed in two (independent) parts—*correctness* and *secrecy*.[2]

Def: Correctness

The protocol is said to be $\varepsilon_{\mathrm{corr}}$-correct if its output satisfies

$$(1 - p_{\perp})\,\Pr[K \neq K'] \leq \varepsilon_{\mathrm{corr}}, \tag{9}$$

where K, K' take values from $\mathcal{K}_{\ell}$.

[2] See Renner PhD Thesis (2005).

The central goal is to establish a tight bound on security error in terms of the protocol parameters (block size, QBER threshold, key length, etc). The security of QKD can be analyzed in two (independent) parts—*correctness* and *secrecy*.[2]

Def: Correctness

The protocol is said to be $\varepsilon_{\text{corr}}$-correct if its output satisfies

$$(1 - p_\perp) \Pr[K \neq K'] \leq \varepsilon_{\text{corr}}, \tag{9}$$

where K, K' take values from $\mathcal{K}_\ell$.

Def: Secrecy

The protocol is said to be ε_{sec}-secret if its output

$$(1 - p_\perp) \frac{1}{2} \|\tilde{\tau}_{KTE} - \omega_K \otimes \tilde{\tau}_{TE}\|_1 \leq \varepsilon_{\text{sec}}. \tag{10}$$

[2] See Renner PhD Thesis (2005).

The central goal is to establish a tight bound on security error in terms of the protocol parameters (block size, QBER threshold, key length, etc). The security of QKD can be analyzed in two (independent) parts—*correctness* and *secrecy*.[2]

Def: Correctness

The protocol is said to be $\varepsilon_{\mathrm{corr}}$-correct if its output satisfies

$$(1 - p_{\perp}) \Pr[K \neq K'] \leq \varepsilon_{\mathrm{corr}}, \tag{9}$$

where K, K' take values from $\mathcal{K}_{\ell}$.

Def: Secrecy

The protocol is said to be $\varepsilon_{\mathrm{sec}}$-secret if its output

$$(1 - p_{\perp}) \frac{1}{2} \|\tilde{\tau}_{KTE} - \omega_K \otimes \tilde{\tau}_{TE}\|_1 \leq \varepsilon_{\mathrm{sec}}. \tag{10}$$

Important: A protocol that is $\varepsilon_{\mathrm{corr}}$-correct and $\varepsilon_{\mathrm{sec}}$-secret is $(\varepsilon_{\mathrm{corr}} + \varepsilon_{\mathrm{sec}})$-secure.

[2] See Renner PhD Thesis (2005).

The goal of *classical post processing* (CPP) is to convert a weakly correlated and weakly secret *raw key*[3] pair, denoted by (X, X'), into an identical secret key pair (K, K').

[3] We define the raw key pair as the measurement data pair after sifting (if needed), just before the parameter estimation step.

The goal of *classical post processing* (CPP) is to convert a weakly correlated and weakly secret *raw key*[3] pair, denoted by (X, X'), into an identical secret key pair (K, K').

[3] We define the raw key pair as the measurement data pair after sifting (if needed), just before the parameter estimation step.

The goal of *classical post processing* (CPP) is to convert a weakly correlated and weakly secret *raw key*[3] pair, denoted by (X, X'), into an identical secret key pair (K, K').

The CPP layer typically consists of the following steps:

1. **Parameter estimation** (sampling error)

[3] We define the raw key pair as the measurement data pair after sifting (if needed), just before the parameter estimation step.

The goal of *classical post processing* (CPP) is to convert a weakly correlated and weakly secret *raw key*[3] pair, denoted by (X, X'), into an identical secret key pair (K, K').

The CPP layer typically consists of the following steps:

1. **Parameter estimation** (sampling error)
2. Information reconciliation & verification (hashing/collision error)

[3] We define the raw key pair as the measurement data pair after sifting (if needed), just before the parameter estimation step.

The goal of *classical post processing* (CPP) is to convert a weakly correlated and weakly secret *raw key*[3] pair, denoted by (X, X'), into an identical secret key pair (K, K').

The CPP layer typically consists of the following steps:

1. **Parameter estimation** (sampling error)
2. Information reconciliation & verification (hashing/collision error)
3. **Privacy amplification** (entropy loss/approximate security)

[3] We define the raw key pair as the measurement data pair after sifting (if needed), just before the parameter estimation step.

The goal of *classical post processing* (CPP) is to convert a weakly correlated and weakly secret *raw key*[3] pair, denoted by (X, X'), into an identical secret key pair (K, K').

The CPP layer typically consists of the following steps:

1. **Parameter estimation** (sampling error)
2. Information reconciliation & verification (hashing/collision error)
3. **Privacy amplification** (entropy loss/approximate security)

In a nutshell, these errors arise from non-asymptotic (finite-length) analyses and can be made arbitrarily small when the underlying sample/block size is sufficiently large.

[3] We define the raw key pair as the measurement data pair after sifting (if needed), just before the parameter estimation step.

The goal of *classical post processing* (CPP) is to convert a weakly correlated and weakly secret *raw key*[3] pair, denoted by (X, X'), into an identical secret key pair (K, K').

The CPP layer typically consists of the following steps:

1. **Parameter estimation** (sampling error)
2. Information reconciliation & verification (hashing/collision error)
3. **Privacy amplification** (entropy loss/approximate security)

In a nutshell, these errors arise from non-asymptotic (finite-length) analyses and can be made arbitrarily small when the underlying sample/block size is sufficiently large.

Basically, the finite-key security of QKD studies the maximization of the extractable secret key length (denoted by ℓ) via the optimisation of these errors and protocol parameters.

[3] We define the raw key pair as the measurement data pair after sifting (if needed), just before the parameter estimation step.

Parameter estimation is needed in QKD to infer the amount of information (of the raw key) that is leaked out to environment (Eve).

Parameter estimation is needed in QKD to infer the amount of information (of the raw key) that is leaked out to environment (Eve).

Basic problem: Suppose a binary sequence $\{w_1, w_2, \ldots, w_N\}$[4] of length N and a random sample of size k is drawn (without replacement). The goal is the infer the number of 1's/errors in the remaining sequence (of size $n = N - k$) by analyzing the statistics of the random sample.

[4]This sequence indicates error positions in the raw key pair (X, X').

Parameter estimation is needed in QKD to infer the amount of information (of the raw key) that is leaked out to environment (Eve).

Basic problem: Suppose a binary sequence $\{w_1, w_2, \ldots, w_N\}$[4] of length N and a random sample of size k is drawn (without replacement). The goal is the infer the number of 1's/errors in the remaining sequence (of size $n = N - k$) by analyzing the statistics of the random sample.

The probability of interest[5] (for a given tolerated error rate δ and non-negative deviation gap ν) is defined as

$$\mathbb{P}_{\mathrm{pe}}(\delta, \nu) := \Pr\left[(\overline{W}_{\mathrm{pe}} \leq \delta) \cap (\overline{W}_{\mathrm{key}} \geq \delta + \nu)\right], \tag{11}$$

where $\overline{W}_{\mathrm{pe}}$ and $\overline{W}_{\mathrm{key}}$ are the random error rates of the random sample and final raw key, respectively.

[4] This sequence indicates error positions in the raw key pair (X, X').

[5] See Tomamichel & Leverrier, Quantum 1, 14 (2017) and Lim et al. Phys. Rev. Lett. 126, 100501 (2021).

The event $(\overline{W}_{\mathsf{pe}} \leq \delta) \cap (\overline{W}_{\mathsf{key}} \geq \delta + \nu)$ defines a bad scenario: the random sample admits an error rate that is smaller than the tolerated error rate and the final raw key contains more errors than allowed.

The event $(\overline{W}_{\text{pe}} \leq \delta) \cap (\overline{W}_{\text{key}} \geq \delta + \nu)$ defines a bad scenario: the random sample admits an error rate that is smaller than the tolerated error rate and the final raw key contains more errors than allowed.

This means that the parameter estimation step has failed and the probability of a bad event happening can be upper bounded by

Lemma: error bound based on Serfling's inequality

$$\mathbb{P}_{\text{pe}}(\delta, \nu) \leq {}^{a} \exp\left(-2\nu^2 \frac{(N-k)k^2}{N(k+1)}\right). \tag{12}$$

[a] Tomamichel, Lim, Gisin & Renner, Nat. Commun. 3, 634 (2012).

The event $(\overline{W}_{\mathrm{pe}} \leq \delta) \cap (\overline{W}_{\mathrm{key}} \geq \delta + \nu)$ defines a bad scenario: the random sample admits an error rate that is smaller than the tolerated error rate and the final raw key contains more errors than allowed.

This means that the parameter estimation step has failed and the probability of a bad event happening can be upper bounded by

Lemma: error bound based on Serfling's inequality

$$\mathbb{P}_{\mathrm{pe}}(\delta, \nu) \leq {}^{a} \exp\left(-2\nu^2 \frac{(N-k)k^2}{N(k+1)}\right). \tag{12}$$

[a] Tomamichel, Lim, Gisin & Renner, Nat. Commun. 3, 634 (2012).

Notice that Serfling's inequality[6] (like Hoeffding's inequality) is pretty general and applies to non-binary valued sequences as well.

[6] Serfling, Ann. Statist. 2, 39–48, (1974).

Clearly, there is interest to further sharpen the upper bound on $\mathbb{P}_{\mathsf{pe}}(\delta, \nu)$.

Clearly, there is interest to further sharpen the upper bound on $\mathbb{P}_{\mathsf{pe}}(\delta, \nu)$.

One way is to exploit the fact that the error distribution of the random sample (drawn without replacement) is given by a *hypergeometric distribution*.

Clearly, there is interest to further sharpen the upper bound on $\mathbb{P}_{\mathrm{pe}}(\delta, \nu)$.

One way is to exploit the fact that the error distribution of the random sample (drawn without replacement) is given by a *hypergeometric distribution*.

Lemma: error bound based on Hush and Scovel's hypergeometric inequality

For any $\nu > \xi > 0$ such that $N(\delta + \xi) \in \mathbb{Z}^+$ and $n^2(\nu - \xi)^2 > 1$,

$$\mathbb{P}_{\mathrm{pe}}(\delta, \nu) \leq {}^{a} \exp\left(-\frac{2Nk\xi^2}{n+1}\right) + \exp\left(-2\Gamma_{N(\delta+\xi)}((n\nu')^2 - 1)\right), \quad (13)$$

where $\nu' := \nu - \xi$ and $\Gamma_{N(\delta+\xi)} := \frac{1}{N(\delta+\xi)+1} + \frac{1}{N-N(\delta+\xi)+1}$.

[a] Lim, Xu, Pan & Ekert. Phys. Rev. Lett. 126, 100501 (2021)

Clearly, there is interest to further sharpen the upper bound on $\mathbb{P}_{\mathrm{pe}}(\delta, \nu)$.

One way is to exploit the fact that the error distribution of the random sample (drawn without replacement) is given by a *hypergeometric distribution*.

Lemma: error bound based on Hush and Scovel's hypergeometric inequality

For any $\nu > \xi > 0$ such that $N(\delta + \xi) \in \mathbb{Z}^+$ and $n^2(\nu - \xi)^2 > 1$,

$$\mathbb{P}_{\mathrm{pe}}(\delta, \nu) \leq {}^{a} \exp\left(-\frac{2Nk\xi^2}{n+1}\right) + \exp\left(-2\Gamma_{N(\delta+\xi)}((n\nu')^2 - 1)\right), \tag{13}$$

where $\nu' := \nu - \xi$ and $\Gamma_{N(\delta+\xi)} := \frac{1}{N(\delta+\xi)+1} + \frac{1}{N-N(\delta+\xi)+1}$.

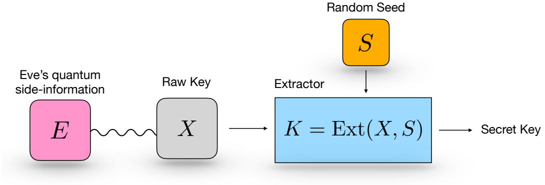
[a] Lim, Xu, Pan & Ekert. Phys. Rev. Lett. 126, 100501 (2021)

Food for thought: It is plausible that the above bound can be further improved using the results in Bancal et al. Quantum 5, 401 (2021) and Yin & Chen, Sci. Rep. 9 17113 (2019).

Roughly speaking, the goal of privacy amplification[7] is to turn a weakly random source X (which is correlated with quantum system E) to one that is *almost* uniform and independent of E.

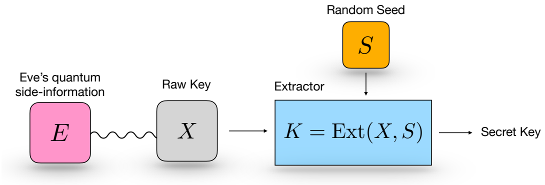
[7] Bennett et al. SIAM J. Comput, 17(2):210-229, (1988); Bennett et al. IEEE Trans. Inf. Th., 41, 6 (1995).

Roughly speaking, the goal of privacy amplification[7] is to turn a weakly random source X (which is correlated with quantum system E) to one that is *almost* uniform and independent of E.



[7] Bennett et al. SIAM J. Comput, 17(2):210-229, (1988); Bennett et al. IEEE Trans. Inf. Th., 41, 6 (1995).

Roughly speaking, the goal of privacy amplification[7] is to turn a weakly random source X (which is correlated with quantum system E) to one that is *almost* uniform and independent of E.



Definition: Quantum-proof strong extractor

A function Ext : $\{0,1\}^n \times \{0,1\}^r \to \{0,1\}^\ell$, is a quantum (k, ε)-*strong extractor*[a] with uniform seed S (r bits), if for any ρ_{XE} with $H_{\min}(X|E) \geq k$, its output satisfies

$$\frac{1}{2}\|\rho_{\mathrm{Ext}(X,S)SE} - \rho_{U_\ell} \otimes \rho_S \otimes \rho_E\|_1 \leq \varepsilon, \tag{14}$$

where U_ℓ is uniform over $\mathcal{K}_\ell$.

[a] See Section 2.6. in Koenig & Renner, IEEE Trans. Inf. Th., 57, 4760 (2011).

[7] Bennett et al. SIAM J. Comput, 17(2):210-229, (1988); Bennett et al. IEEE Trans. Inf. Th., 41, 6 (1995).

Key points for tutorial:

- Two-universal hashing[8] can be used to build quantum-proof strong extractors[9].

[8] A family $\mathcal{F}$ of hash functions taking $\{0,1\}^n \rightarrow \{0,1\}^m$ is called universal if for any randomly chosen function f from the family and $x \neq y$, $\Pr[f(x) = f(y)] \leq 1/2^m$.

[9] Renner PhD Thesis (2005); see Corollary 5.6.1.

Key points for tutorial:

- Two-universal hashing[8] can be used to build quantum-proof strong extractors[9].
- Smooth min-entropy of X given E is the relevant measure of extractable private randomness[10].

[8] A family $\mathcal{F}$ of hash functions taking $\{0,1\}^n \rightarrow \{0,1\}^m$ is called universal if for any randomly chosen function f from the family and $x \neq y$, $\Pr[f(x) = f(y)] \leq 1/2^m$.

[9] Renner PhD Thesis (2005); see Corollary 5.6.1.

[10] See Koenig, Renner, & Schaffner, IEEE Trans. Inf. Th., 55, 9 (2009).

Key points for tutorial:

- Two-universal hashing[8] can be used to build quantum-proof strong extractors[9].
- Smooth min-entropy of X given E is the relevant measure of extractable private randomness[10].

Lemma: leftover hashing against quantum side-information

Let ρ_{XE} be a classical-quantum state and $\mathcal{F} = \{f_s : \{0,1\}^n \to \{0,1\}^\ell\}$ be a universal family with $Z = f_s(X)$. Then[a],

$$\Delta_t(\rho_{ZSE}, \rho_{U_\ell} \otimes \rho_S \otimes \rho_E) \leq \frac{1}{2}\sqrt{2^{\ell - H_{\min}^{\varepsilon_1}(X|E)_\rho}} + \varepsilon_1. \quad (15)$$

[a] Renner PhD Thesis (2005); see Corollary 5.6.1.

[8] A family $\mathcal{F}$ of hash functions taking $\{0,1\}^n \to \{0,1\}^m$ is called universal if for any randomly chosen function f from the family and $x \neq y$, $\Pr[f(x) = f(y)] \leq 1/2^m$.

[9] Renner PhD Thesis (2005); see Corollary 5.6.1.

[10] See Koenig, Renner, & Schaffner, IEEE Trans. Inf. Th., 55, 9 (2009).

Key points for tutorial:

- Two-universal hashing[8] can be used to build quantum-proof strong extractors[9].
- Smooth min-entropy of X given E is the relevant measure of extractable private randomness[10].

Lemma: leftover hashing against quantum side-information

Let ρ_{XE} be a classical-quantum state and $\mathcal{F} = \{f_s : \{0,1\}^n \to \{0,1\}^\ell\}$ be a universal family with $Z = f_s(X)$. Then[a],

$$\Delta_t(\rho_{ZSE}, \rho_{U_\ell} \otimes \rho_S \otimes \rho_E) \leq \frac{1}{2}\sqrt{2^{\ell - H_{\min}^{\varepsilon_1}(X|E)_\rho}} + \varepsilon_1. \tag{15}$$

[a] Renner PhD Thesis (2005); see Corollary 5.6.1.

Impt: Pick the right output length ℓ:

$$\ell = \left\lfloor H_{\min}^{\varepsilon_1}(X|E)_\rho - 2\log_2 \frac{1}{2\varepsilon_2} \right\rfloor \Rightarrow \Delta_t(\rho_{ZSE}, \rho_{U_\ell} \otimes \rho_S \otimes \rho_E) \leq \varepsilon_1 + \varepsilon_2.$$

[8] A family $\mathcal{F}$ of hash functions taking $\{0,1\}^n \to \{0,1\}^m$ is called universal if for any randomly chosen function f from the family and $x \neq y$, $\Pr[f(x) = f(y)] \leq 1/2^m$.

[9] Renner PhD Thesis (2005); see Corollary 5.6.1.

[10] See Koenig, Renner, & Schaffner, IEEE Trans. Inf. Th., 55, 9 (2009).

Comparing the secrecy condition, Eq. (10), and Eq. (15), we see that privacy amplification via universal hashing guarantees $\varepsilon_{\rm sec}$-secrecy if $\varepsilon_1 + \varepsilon_2 \leq \varepsilon_{\rm sec}$ and if the (smooth) min-entropy of X given TE[11] is known:

$$H_{\min}^{\varepsilon_1}(X|TE)_\rho \geq \text{fill-in-the-blank}.$$

[11] Recall that T is the classical information exchanged over the CPP phase.

[12] Toyohiro Tsurumaru, Equivalence of three classical algorithms with quantum side information: Privacy amplification, error correction, and data compression, arXiv:2009.08823.

Comparing the secrecy condition, Eq. (10), and Eq. (15), we see that privacy amplification via universal hashing guarantees $\varepsilon_{\rm sec}$-secrecy if $\varepsilon_1 + \varepsilon_2 \leq \varepsilon_{\rm sec}$ and if the (smooth) min-entropy of X given TE[11] is known:

$$H_{\min}^{\varepsilon_1}(X|TE)_\rho \geq \text{fill-in-the-blank}.$$

- Traditionally, two broad approaches: (a) Information-theoretic approach and (b) entanglement distillation approach.

[11] Recall that T is the classical information exchanged over the CPP phase.

[12] Toyohiro Tsurumaru, Equivalence of three classical algorithms with quantum side information: Privacy amplification, error correction, and data compression, arXiv:2009.08823.

Comparing the secrecy condition, Eq. (10), and Eq. (15), we see that privacy amplification via universal hashing guarantees ε_{sec}-secrecy if $\varepsilon_1 + \varepsilon_2 \leq \varepsilon_{\text{sec}}$ and if the (smooth) min-entropy of X given TE[11] is known:

$$H_{\min}^{\varepsilon_1}(X|TE)_\rho \geq \text{fill-in-the-blank}.$$

- Traditionally, two broad approaches: (a) Information-theoretic approach and (b) entanglement distillation approach.
- Recently, it has been clarified that these two approaches are essentially the same (except for some constant prefactor in the secrecy condition); see poster #67 by Toyohiro Tsurumaru[12]

[11] Recall that T is the classical information exchanged over the CPP phase.

[12] Toyohiro Tsurumaru, Equivalence of three classical algorithms with quantum side information: Privacy amplification, error correction, and data compression, arXiv:2009.08823.

Comparing the secrecy condition, Eq. (10), and Eq. (15), we see that privacy amplification via universal hashing guarantees $\varepsilon_{\rm sec}$-secrecy if $\varepsilon_1 + \varepsilon_2 \leq \varepsilon_{\rm sec}$ and if the (smooth) min-entropy of X given TE[11] is known:

$$H_{\min}^{\varepsilon_1}(X|TE)_\rho \geq \text{fill-in-the-blank}.$$

- Traditionally, two broad approaches: (a) Information-theoretic approach and (b) entanglement distillation approach.
- Recently, it has been clarified that these two approaches are essentially the same (except for some constant prefactor in the secrecy condition); see poster #67 by Toyohiro Tsurumaru[12]
- In general, the direct computation of smooth min-entropy is an open question—even in the case of qubit channels, the set of compatible bipartite states (for typical block sizes $\sim 10^4$ - 10^9) is impossible to characterise.

[11] Recall that T is the classical information exchanged over the CPP phase.

[12] Toyohiro Tsurumaru, Equivalence of three classical algorithms with quantum side information: Privacy amplification, error correction, and data compression, arXiv:2009.08823.

It has been observed (for some protocols) that it is sufficient to consider security against collective attacks[13] in the asymptotic limit.

[13] In this case, the bipartite state of interest $\rho_{XE} = \rho_{X_1E_1} \otimes \rho_{X_2E_2} \otimes \ldots \rho_{X_nE_n}$ assumes a tensor product form.

It has been observed (for some protocols) that it is sufficient to consider security against collective attacks[13] in the asymptotic limit.

In the finite-key regime, the validity of this observation is more involved but pretty good proof strategies exist.

[13] In this case, the bipartite state of interest $\rho_{XE} = \rho_{X_1 E_1} \otimes \rho_{X_2 E_2} \otimes \ldots \rho_{X_n E_n}$ assumes a tensor product form.

It has been observed (for some protocols) that it is sufficient to consider security against collective attacks[13] in the asymptotic limit.

In the finite-key regime, the validity of this observation is more involved but pretty good proof strategies exist.

- Proof techniques that offer **direct bounding of smooth min-entropies**.
  - Uncertainty relations for smooth min-entropies: Tomamichel & Renner, Phys. Rev. Lett. 106, 110506 (2011); Tomamichel, Lim, Gisin & Renner, Nat. Commun. 3, 634 (2012); Furrer et. al, Phys. Rev. Lett. 109, 100502 (2012); Lim et al. Phys. Rev. A 89, 022307 (2014); Tomamichel & Leverrier, Quantum 1, 14 (2017).
  - See also the presentations (contributed talks 2a #1 and 5b #3) by Nitin Jain & Jasminder Sidhu, respectively.

[13] In this case, the bipartite state of interest $\rho_{XE} = \rho_{X_1E_1} \otimes \rho_{X_2E_2} \otimes \ldots \rho_{X_nE_n}$ assumes a tensor product form.

It has been observed (for some protocols) that it is sufficient to consider security against collective attacks[13] in the asymptotic limit.

In the finite-key regime, the validity of this observation is more involved but pretty good proof strategies exist.

- Proof techniques that offer **direct bounding of smooth min-entropies**.
  - Uncertainty relations for smooth min-entropies: Tomamichel & Renner, Phys. Rev. Lett. 106, 110506 (2011); Tomamichel, Lim, Gisin & Renner, Nat. Commun. 3, 634 (2012); Furrer et. al, Phys. Rev. Lett. 109, 100502 (2012); Lim et al. Phys. Rev. A 89, 022307 (2014); Tomamichel & Leverrier, Quantum 1, 14 (2017).
  - See also the presentations (contributed talks 2a #1 and 5b #3) by Nitin Jain & Jasminder Sidhu, respectively.
- Proof techniques that **promote collective attacks bounds to general attacks bounds**.
  - Quantum de Finetti theorems (exponential/postselection): Renner, Ph.D. thesis (2005); Christandl, Koenig, & Renner, Phys. Rev. Lett. 102, 020504 (2009); Leverrier et al., Phys. Rev. Lett. 110, 030502 (2013); Leverrier, Phys. Rev. Lett. 118, 200501 (2017).

[13] In this case, the bipartite state of interest $\rho_{XE} = \rho_{X_1E_1} \otimes \rho_{X_2E_2} \otimes \dots \rho_{X_nE_n}$ assumes a tensor product form.

It has been observed (for some protocols) that it is sufficient to consider security against collective attacks[13] in the asymptotic limit.

In the finite-key regime, the validity of this observation is more involved but pretty good proof strategies exist.

- Proof techniques that offer **direct bounding of smooth min-entropies**.
  - Uncertainty relations for smooth min-entropies: Tomamichel & Renner, Phys. Rev. Lett. 106, 110506 (2011); Tomamichel, Lim, Gisin & Renner, Nat. Commun. 3, 634 (2012); Furrer et. al, Phys. Rev. Lett. 109, 100502 (2012); Lim et al. Phys. Rev. A 89, 022307 (2014); Tomamichel & Leverrier, Quantum 1, 14 (2017).
  - See also the presentations (contributed talks 2a #1 and 5b #3) by Nitin Jain & Jasminder Sidhu, respectively.
- Proof techniques that **promote collective attacks bounds to general attacks bounds**.
  - Quantum de Finetti theorems (exponential/postselection): Renner, Ph.D. thesis (2005); Christandl, Koenig, & Renner, Phys. Rev. Lett. 102, 020504 (2009); Leverrier et al., Phys. Rev. Lett. 110, 030502 (2013); Leverrier, Phys. Rev. Lett. 118, 200501 (2017).
  - Entropy accumulation theorem (EAT): Dupuis, Fawzi & Renner, Commun. Math. Phys. 379, 867–913 (2020); Arnon-Friedman et al. Nat Commun 9, 459 (2018); Schwonnek et al. Nat Commun 12, 2880 (2021).
  - See also the presentation (contributed talk 2b #2) by Ernest Tan.

[13] In this case, the bipartite state of interest $\rho_{XE} = \rho_{X_1 E_1} \otimes \rho_{X_2 E_2} \otimes \ldots \rho_{X_n E_n}$ assumes a tensor product form.

Example 1: finite-key security of BBM92

Security based on entropic uncertainty relations (part 1)

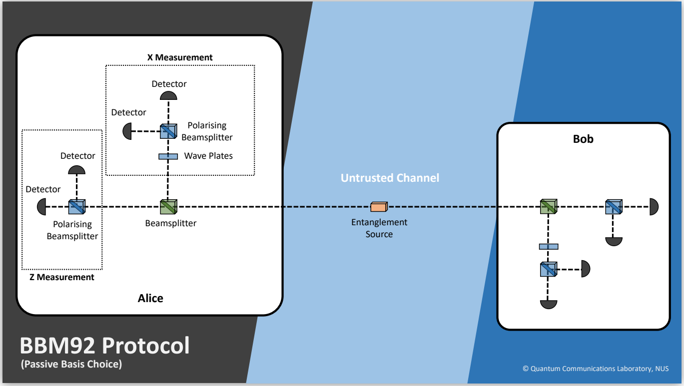


Figure: Bennett-Brassard-Mermin 1992 (BBM92) Entanglement-based QKD with passive-basis choice

Important assumptions:

- Untrusted source but measurements must be trusted (squashing model is required).
- The POVM elements corresponding to the inconclusive outcome are identical.

Protocol settings (block size m, random sample size k, deviation δ, syndrome size r, hash size t, and output key size ℓ):

Protocol settings (block size m, random sample size k, deviation δ, syndrome size r, hash size t, and output key size ℓ):

1. Measurement. Alice and Bob agree on a random binary string $\Phi \in \{0,1\}^m$ over an authenticated public channel and measure their respective quantum signals using this string. They then agree on a random sample (drawn without replacement) of size k from the entire measurement data set and store them into two pairs of strings: (X, V) for Alice and (Y, W) for Bob. Here, X and Y are random strings taking values in $\{0,1\}^n$; thus V and W take values in $\{0,1\}^k$. Note that $m = n + k$.

Protocol settings (block size m, random sample size k, deviation δ, syndrome size r, hash size t, and output key size ℓ):

1. Measurement. Alice and Bob agree on a random binary string $\Phi \in \{0,1\}^m$ over an authenticated public channel and measure their respective quantum signals using this string. They then agree on a random sample (drawn without replacement) of size k from the entire measurement data set and store them into two pairs of strings: (X, V) for Alice and (Y, W) for Bob. Here, X and Y are random strings taking values in $\{0,1\}^n$; thus V and W take values in $\{0,1\}^k$. Note that $m = n + k$.

2. Parameter estimation. Alice publicly sends V to Bob, who then computes the error rate between V and W, i.e., $\overline{Z}_{\mathrm{pe}} := |V \oplus W|/k$. If the error rate exceeds the tolerated error rate δ, they abort the protocol. Otherwise, they proceed to the next step. This decision is stored in a binary-valued flag $F_{\mathrm{pe}} \in \{\checkmark, \varnothing\}$, where $\checkmark$ means successful and $\varnothing$ means abort.

Protocol settings (block size m, random sample size k, deviation δ, syndrome size r, hash size t, and output key size ℓ):

1. Measurement. Alice and Bob agree on a random binary string $\Phi \in \{0,1\}^m$ over an authenticated public channel and measure their respective quantum signals using this string. They then agree on a random sample (drawn without replacement) of size k from the entire measurement data set and store them into two pairs of strings: (X, V) for Alice and (Y, W) for Bob. Here, X and Y are random strings taking values in $\{0,1\}^n$; thus V and W take values in $\{0,1\}^k$. Note that $m = n + k$.

2. Parameter estimation. Alice publicly sends V to Bob, who then computes the error rate between V and W, i.e., $\overline{Z}_{\mathrm{pe}} := |V \oplus W|/k$. If the error rate exceeds the tolerated error rate δ, they abort the protocol. Otherwise, they proceed to the next step. This decision is stored in a binary-valued flag $F_{\mathrm{pe}} \in \{\checkmark, \varnothing\}$, where $\checkmark$ means successful and $\varnothing$ means abort.

3. One-way error correction. Alice sends Bob a syndrome T of length r which is computed from her raw key X. Then Bob generates an estimate of Alice's raw key, X', from Y and T. To verify that the correction is successful, Alice computes a hash $H(X)$ (of length t) of X and sends it to Bob, who then compares it with his hash $H(X')$. If the hash values are different (i.e., $H(X) \neq H(X')$), they abort the protocol; this decision is stored in $F_{\mathrm{ec}} \in \{\checkmark, \varnothing\}$.

Protocol settings (block size m, random sample size k, deviation δ, syndrome size r, hash size t, and output key size ℓ):

1. Measurement. Alice and Bob agree on a random binary string $\Phi \in \{0,1\}^m$ over an authenticated public channel and measure their respective quantum signals using this string. They then agree on a random sample (drawn without replacement) of size k from the entire measurement data set and store them into two pairs of strings: (X, V) for Alice and (Y, W) for Bob. Here, X and Y are random strings taking values in $\{0,1\}^n$; thus V and W take values in $\{0,1\}^k$. Note that $m = n + k$.

2. Parameter estimation. Alice publicly sends V to Bob, who then computes the error rate between V and W, i.e., $\overline{Z}_{\mathrm{pe}} := |V \oplus W|/k$. If the error rate exceeds the tolerated error rate δ, they abort the protocol. Otherwise, they proceed to the next step. This decision is stored in a binary-valued flag $F_{\mathrm{pe}} \in \{\checkmark, \varnothing\}$, where $\checkmark$ means successful and $\varnothing$ means abort.

3. One-way error correction. Alice sends Bob a syndrome T of length r which is computed from her raw key X. Then Bob generates an estimate of Alice's raw key, X', from Y and T. To verify that the correction is successful, Alice computes a hash $H(X)$ (of length t) of X and sends it to Bob, who then compares it with his hash $H(X')$. If the hash values are different (i.e., $H(X) \neq H(X')$), they abort the protocol; this decision is stored in $F_{\mathrm{ec}} \in \{\checkmark, \varnothing\}$.

4. Privacy Amplification. Alice and Bob perform randomness extraction based on two-universal hashing to extract an identical secret key pair, K and K', each of length ℓ, from X and X', respectively.

Thm: Security bound

For the QKD protocol described above with fixed settings, it is $\varepsilon_{\rm qkd}$-secure if there exists $\nu \in (0, 1/2 - \delta]$ satisfying[a]

$$\underbrace{2^{-t}}_{\text{VER error}} + \underbrace{2\varepsilon_{\rm pe}(\nu)}_{\text{PE error}} + \underbrace{\varepsilon_{\rm pa}(\nu)}_{\text{PA error}} \leq \varepsilon_{\rm qkd}, \tag{16}$$

where the error functions due to privacy amplification and parameter estimation are defined as

$$\begin{aligned} \varepsilon_{\rm pa}(\nu) &:= \frac{1}{2}\sqrt{2^{-n[1-h_2(\delta+\nu)]+r+t+\ell}}, \\ \varepsilon_{\rm pe}(\nu) &:= \exp\left(-\frac{nk^2\nu^2}{m(k+1)}\right), \end{aligned}$$

respectively, and with $h_2(x) := -x\log x - (1-x)\log(1-x)$, the binary entropy function.

[a] See Lim, Xu, Pan & Ekert. Phys. Rev. Lett. 126, 100501 (2021); readapted from Tomamichel & Leverrier, Quantum 1, 14 (2017).

Example 1: finite-key security of BBM92

Security based on entropic uncertainty relations (part 3)

Thm: Security bound

For the QKD protocol described above with fixed settings, it is $\varepsilon_{\mathrm{qkd}}$-secure if there exists $\nu \in (0, 1/2 - \delta]$ satisfying[a]

$$\underbrace{2^{-t}}_{\text{VER error}} + \underbrace{2\varepsilon_{\mathrm{pe}}(\nu)}_{\text{PE error}} + \underbrace{\varepsilon_{\mathrm{pa}}(\nu)}_{\text{PA error}} \leq \varepsilon_{\mathrm{qkd}}, \tag{16}$$

where the error functions due to privacy amplification and parameter estimation are defined as

$$\begin{aligned} \varepsilon_{\mathrm{pa}}(\nu) &:= \frac{1}{2}\sqrt{2^{-n[1-h_2(\delta+\nu)]+r+t+\ell}}, \\ \varepsilon_{\mathrm{pe}}(\nu) &:= \exp\left(-\frac{nk^2\nu^2}{m(k+1)}\right), \end{aligned}$$

respectively, and with $h_2(x) := -x\log x - (1-x)\log(1-x)$, the binary entropy function.

[a] See Lim, Xu, Pan & Ekert. Phys. Rev. Lett. 126, 100501 (2021); readapted from Tomamichel & Leverrier, Quantum 1, 14 (2017).

Impt: The sampling error above is based on Serfling's inequality, Eq. (12), and can be tighten using Eq. (13).

Example 1: finite-key security of BBM92

Security based on entropic uncertainty relations (part 4)

Optimisation program

To maximize ℓ, consider a program parameterized by a bounded set of four-dimensional real vector, $\vec{x} = (\alpha, \beta, \nu, \xi)$. The block length m, tolerated error rate δ, correctness error $2^{-t} = 10^{-(s+2)}$, and security parameter $\varepsilon_{\rm qkd} = 10^{-s}$ are fixed.

$$\begin{aligned} \max_{\vec{x}\in\mathbb{R}^4} \quad & \ell = \lfloor \alpha m \rfloor \\ \text{s.t.} \quad & 2^{-t} + 2\varepsilon'_{\rm pe}(\nu,\xi) + \varepsilon_{\rm pa}(\nu) \leq \varepsilon_{\rm qkd}, \\ & \alpha \in [0,1], \beta \in (0, 1/2], \\ & 0 < \xi < \nu < 1/2 - \delta, \end{aligned}$$

where $k = \lfloor \beta m \rfloor$ is the number of bits allocated to parameter estimation and $r = 1.19 h_2(\delta)$ is the expected error correction leakage.

- The secret key rate is $\alpha := \ell/m$, the number of extractable secret bits divided by block size.
- The correctness is always two orders of magnitude smaller than $\varepsilon_{\rm qkd}$.
- We apply this analysis to the BBM92 QKD experiment data from Yin et. el. Nature 582, 501–505 (2020).

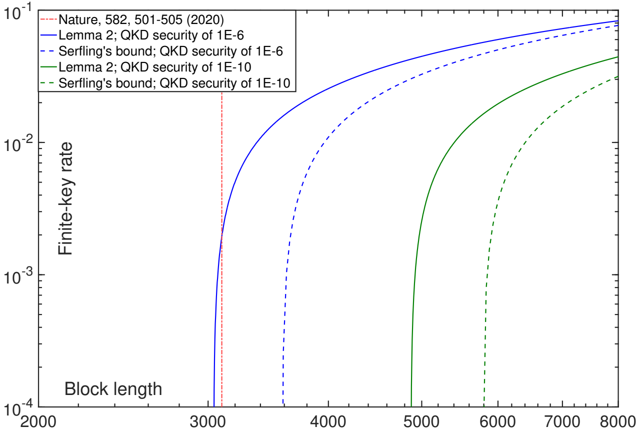


Figure: Numerically optimized finite-key rate ℓ/m vs block length m for $s = 6, 10$. In this simulation, the tolerated error rate is set to $\delta = 4.51\%$. The (red) vertical line represents the block length ($m = 3100$ bits) obtained in the Micius QKD experiment, which gives a finite-key rate of 1.962×10^{-3} based on $\varepsilon_{\mathrm{qkd}} = 10^{-6}$. The optimized parameters are $\vec{x}_{\mathrm{opt}} = \{1.962 \times 10^{-3}, 0.5, 0.1141, 0.0693\}$.

Given there are pretty good proof techniques for converting collective attacks bounds to general attacks bounds, it is of interest to explore methods that would give tight bounds on single-round entropy.

Given there are pretty good proof techniques for converting collective attacks bounds to general attacks bounds, it is of interest to explore methods that would give tight bounds on single-round entropy.

The relevant measure is given by the conditional von Neumann entropy of X_i given E_i:

$$H(X_i|E_i) \geq \text{fill-in-the-blank}$$

Numerical methods for QKD

Let the computer do the job—be it device-dependent or device-independent

Given there are pretty good proof techniques for converting collective attacks bounds to general attacks bounds, it is of interest to explore methods that would give tight bounds on single-round entropy.

The relevant measure is given by the conditional von Neumann entropy of X_i given E_i:

$$H(X_i|E_i) \geq \text{fill-in-the-blank}$$

There are now quite a few methods to compute numerically such lower bounds:

- Coles, Metodiev & Lütkenhaus. Nat Commun 7, 11712 (2016); device-dependent
- Winick, Lütkenhaus & Coles. Quantum 2, 77 (2018); device-dependent
- Hu et al. arXiv:2104.03847 (2021); device-dependent (see poster #216)

Numerical methods for QKD

Let the computer do the job—be it device-dependent or device-independent

Given there are pretty good proof techniques for converting collective attacks bounds to general attacks bounds, it is of interest to explore methods that would give tight bounds on single-round entropy.

The relevant measure is given by the conditional von Neumann entropy of X_i given E_i:

$$H(X_i|E_i) \geq \text{fill-in-the-blank}$$

There are now quite a few methods to compute numerically such lower bounds:

- Coles, Metodiev & Lütkenhaus. Nat Commun 7, 11712 (2016); device-dependent
- Winick, Lütkenhaus & Coles. Quantum 2, 77 (2018); device-dependent
- Hu et al. arXiv:2104.03847 (2021); device-dependent (see poster #216)
- Wang et al. npj Quantum Information 5, 1–6, (2019); one-sided device-independent
- Primaatmaja et al. Phys. Rev. A 99, 062332 (2019); measurement-device-independent
- Bourassa et al. Phys. Rev. A 102, 062607 (2020); measurement-device-independent

Numerical methods for QKD

Let the computer do the job—be it device-dependent or device-independent

Given there are pretty good proof techniques for converting collective attacks bounds to general attacks bounds, it is of interest to explore methods that would give tight bounds on single-round entropy.

The relevant measure is given by the conditional von Neumann entropy of X_i given E_i:

$$H(X_i|E_i) \geq \text{fill-in-the-blank}$$

There are now quite a few methods to compute numerically such lower bounds:

- Coles, Metodiev & Lütkenhaus. Nat Commun 7, 11712 (2016); device-dependent
- Winick, Lütkenhaus & Coles. Quantum 2, 77 (2018); device-dependent
- Hu et al. arXiv:2104.03847 (2021); device-dependent (see poster #216)
- Wang et al. npj Quantum Information 5, 1–6, (2019); one-sided device-independent
- Primaatmaja et al. Phys. Rev. A 99, 062332 (2019); measurement-device-independent
- Bourassa et al. Phys. Rev. A 102, 062607 (2020); measurement-device-independent
- Tan et al. arXiv:1908.11372 (2019); device-independent
- Brown, Fawzi, & Fawzi. Nat Commun 12, 575 (2021); device-independent
- Schwonnek et al. Nat Commun 12, 2880 (2021); device-independent
- Brown, Fawzi, & Fawzi. arXiv:2106.13692 (2021)[14]; device-independent

[14] See presentation (contributed talk 3a #3) by Peter Brown.

Let's focus on measurement-device-independent QKD (MDI-QKD)[15]

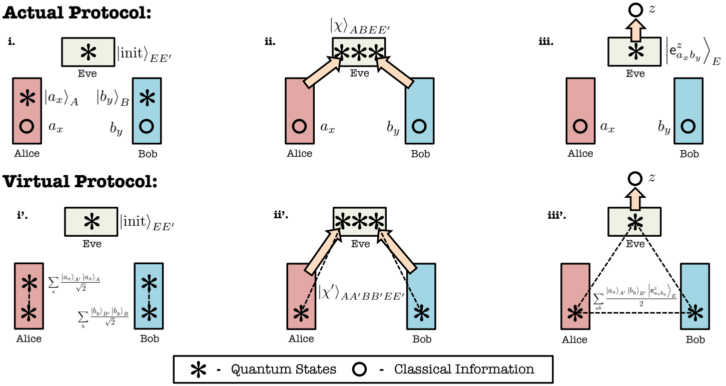


Figure: Virtual protocol for arbitrary MDI-QKD protocols.

[15] See Lo, Curty & Bing Phys. Rev. Lett. 108, 130503 (2012) and Braunstein & Pirandola Phys. Rev. Lett. 108, 130502 (2012).

Let the quantum states prepared by Alice and Bob be denoted by $\{|\mathrm{a}(a_x)\rangle_A\}_{a_x}$ and $\{|\mathrm{b}(b_y)\rangle_B\}_{b_y}$, respectively, where a and b are the bit values while x and y are the corresponding basis choices.

Let the quantum states prepared by Alice and Bob be denoted by $\{|\mathrm{a}(a_x)\rangle_A\}_{a_x}$ and $\{|\mathrm{b}(b_y)\rangle_B\}_{b_y}$, respectively, where a and b are the bit values while x and y are the corresponding basis choices.

The untrusted quantum channel and central measurement can be collectively viewed as a quantum-to-classical map:

$$|\mathrm{a}(a_x)\rangle_A|\mathrm{b}(b_y)\rangle_B \rightarrow \underbrace{\sum_z \left|\mathrm{e}^z_{a_x b_y}\right\rangle_E}_{\text{Eve's quantum information}} |z\rangle_{E'}, \tag{17}$$

where z is the classical announcement made by the central node.

Let the quantum states prepared by Alice and Bob be denoted by $\{|\mathrm{a}(a_x)\rangle_A\}_{a_x}$ and $\{|\mathrm{b}(b_y)\rangle_B\}_{b_y}$, respectively, where a and b are the bit values while x and y are the corresponding basis choices.

The untrusted quantum channel and central measurement can be collectively viewed as a quantum-to-classical map:

$$|\mathrm{a}(a_x)\rangle_A|\mathrm{b}(b_y)\rangle_B \to \underbrace{\sum_z \left|\mathrm{e}^z_{a_x b_y}\right\rangle_E}_{\text{Eve's quantum information}} |z\rangle_{E'}, \tag{17}$$

where z is the classical announcement made by the central node.

The key observation here is that Eve's quantum information forms a Gram matrix G whose entries are constrained by the expected channel parameters and inner-product information of the encoding states:

$$\begin{aligned} \Lambda_{a_x b_y, a'_{x'}, b'_{y'}} &= \underbrace{\left\langle \mathrm{a}(a_x) \middle| \mathrm{a}(a'_{x'}) \right\rangle_A}_{\text{Alice's IP info}} \underbrace{\left\langle \mathrm{b}(b_y) \middle| \mathrm{b}(b'_{y'}) \right\rangle_B}_{\text{Bob's IP info}} \\ &= \sum_z \underbrace{\left\langle \mathrm{e}^z_{a_x b_y} \middle| \mathrm{e}^z_{a'_{x'}, b'_{y'}} \right\rangle_E}_{\text{Eve's IP info}}. \end{aligned} \tag{18}$$

The channel parameters like detection probabilities and error rates are characterized by

$$
\begin{aligned}
P^{\gamma}_{\text{pass}} &= \sum_{a,b} \frac{P(a_\gamma, b_\gamma)}{f_\gamma} P(\text{pass}|a_\gamma, b_\gamma) \\
&= \sum_{a,b} \frac{P(a_\gamma, b_\gamma)}{f_\gamma} \left\langle \mathrm{e}^{\text{pass}}_{a_\gamma b_\gamma} \middle| \mathrm{e}^{\text{pass}}_{a_\gamma b_\gamma} \right\rangle_E \qquad (19)
\end{aligned}
$$

where f_γ is the probability of Alice and Bob both choosing the γ basis and $P(a_\gamma, b_\gamma)$ is the joint probability that Alice chooses a_γ and Bob chooses b_γ.

The channel parameters like detection probabilities and error rates are characterized by

$$\begin{aligned} P^{\gamma}_{\text{pass}} &= \sum_{a,b} \frac{P(a_\gamma, b_\gamma)}{f_\gamma} P(\text{pass}|a_\gamma, b_\gamma) \\ &= \sum_{a,b} \frac{P(a_\gamma, b_\gamma)}{f_\gamma} \left\langle e^{\text{pass}}_{a_\gamma b_\gamma} \middle| e^{\text{pass}}_{a_\gamma b_\gamma} \right\rangle_E \end{aligned} \tag{19}$$

where f_γ is the probability of Alice and Bob both choosing the γ basis and $P(a_\gamma, b_\gamma)$ is the joint probability that Alice chooses a_γ and Bob chooses b_γ.

Similarly, the bit-error rate in the γ basis, denoted by e^{γ}_{bit}, can be expressed as

$$\begin{aligned} e^{\gamma}_{\text{bit}} &= P(a \neq b|\text{pass}, x = y = \gamma) \\ &= \sum_{a \neq b} \frac{P(a_\gamma, b_\gamma)}{P^{\gamma}_{\text{pass}} f_\gamma} P(\text{pass}|a_\gamma, b_\gamma) \\ &= \sum_{a \neq b} \frac{P(a_\gamma, b_\gamma)}{P^{\gamma}_{\text{pass}} f_\gamma} \left\langle e^{\text{pass}}_{a_\gamma b_\gamma} \middle| e^{\text{pass}}_{a_\gamma b_\gamma} \right\rangle_E \end{aligned} \tag{20}$$

where the first equality is from the definition of bit-error rate and the second equality can be easily obtained by applying Bayes rule.

In the asymptotic limit, the secret key rate of the protocol is given by

$$R \geq P_{\text{pass}} \Big[\underbrace{1 - h_2(e_{\text{ph}})}_{\text{Priv. Amp.}} - \underbrace{h_2(e_{\text{bit}})}_{\text{EC leakage}} \Big]. \tag{21}$$

- The bit error rate e_{bit} is generally fixed in optimisation; one can observe this directly in experiments.

In the asymptotic limit, the secret key rate of the protocol is given by

$$R \geq P_{\text{pass}} \Big[\underbrace{1 - h_2(e_{\text{ph}})}_{\text{Priv. Amp.}} - \underbrace{h_2(e_{\text{bit}})}_{\text{EC leakage}} \Big]. \tag{21}$$

- The bit error rate e_{bit} is generally fixed in optimisation; one can observe this directly in experiments.
- The phase error rate e_{ph} is a hypothetical parameter and can only be virtually estimated; it needs to be maximized (using semidefinite programming) over all compatible purified states.

In the asymptotic limit, the secret key rate of the protocol is given by

$$R \geq P_{\text{pass}} \Big[\underbrace{1 - h_2(e_{\text{ph}})}_{\text{Priv. Amp.}} - \underbrace{h_2(e_{\text{bit}})}_{\text{EC leakage}} \Big]. \tag{21}$$

- The bit error rate e_{bit} is generally fixed in optimisation; one can observe this directly in experiments.
- The phase error rate e_{ph} is a hypothetical parameter and can only be virtually estimated; it needs to be maximized (using semidefinite programming) over all compatible purified states.

$$\begin{aligned}
\texttt{maximize} \quad & e_{\text{ph}} \\
\texttt{s.t} \quad & G \succeq 0 \\
& e_{\text{ph}} \leq 1/2 \\
& P^{\gamma}_{\text{pass}} = \sum_{a,b} \frac{P(a_\gamma, b_\gamma)}{f_\gamma} \left\langle \mathrm{e}^{\text{pass}}_{a_\gamma b_\gamma} \middle| \mathrm{e}^{\text{pass}}_{a_\gamma b_\gamma} \right\rangle_E \\
& e^{\gamma}_{\text{bit}} = \sum_{a \neq b} \frac{P(a_\gamma, b_\gamma)}{P^{\gamma}_{\text{pass}} f_\gamma} \left\langle \mathrm{e}^{\text{pass}}_{a_\gamma b_\gamma} \middle| \mathrm{e}^{\text{pass}}_{a_\gamma b_\gamma} \right\rangle_E \\
& \Lambda_{a_x b_y, a'_{x'}, b'_{y'}} = \sum_z \left\langle \mathrm{e}^z_{a_x b_y} \middle| \mathrm{e}^z_{a'_{x'}, b'_{y'}} \right\rangle_E .
\end{aligned} \tag{22}$$

The method is **highly versatile** as it requires only the users to define the inner products of the encoding states (including any conceivable side-channel signals).

This naturally allows one to analyze a large family of **realistic transmitter side-channel/noise problems**:

- Mixed-state MDI-QKD; Bourassa et al. Phys. Rev. A 102, 062607 (2020).

The method is **highly versatile** as it requires only the users to define the inner products of the encoding states (including any conceivable side-channel signals).

This naturally allows one to analyze a large family of **realistic transmitter side-channel/noise problems**:

- Mixed-state MDI-QKD; Bourassa et al. Phys. Rev. A 102, 062607 (2020).
- Coherent-state MDIQKD secure against arbitrary Trojan-horse attacks; Zhang et al. PRX Quantum 2, 030304 (2021).

The method is **highly versatile** as it requires only the users to define the inner products of the encoding states (including any conceivable side-channel signals).

This naturally allows one to analyze a large family of **realistic transmitter side-channel/noise problems**:

- Mixed-state MDI-QKD; Bourassa et al. Phys. Rev. A 102, 062607 (2020).
- Coherent-state MDIQKD secure against arbitrary Trojan-horse attacks; Zhang et al. PRX Quantum 2, 030304 (2021).
- Discrete phase randomization TF-QKD; Curras-Lorenzo et al. Phys. Rev. Applied 15, 014016 (2021).

The method is **highly versatile** as it requires only the users to define the inner products of the encoding states (including any conceivable side-channel signals).

This naturally allows one to analyze a large family of **realistic transmitter side-channel/noise problems**:

- Mixed-state MDI-QKD; Bourassa et al. Phys. Rev. A 102, 062607 (2020).
- Coherent-state MDIQKD secure against arbitrary Trojan-horse attacks; Zhang et al. PRX Quantum 2, 030304 (2021).
- Discrete phase randomization TF-QKD; Curras-Lorenzo et al. Phys. Rev. Applied 15, 014016 (2021).
- MDI-QKD with passive time-dependent source side-channels; Bourassa et al. arXiv:2108.08698 (2021); see poster # 135.

The method is **highly versatile** as it requires only the users to define the inner products of the encoding states (including any conceivable side-channel signals).

This naturally allows one to analyze a large family of **realistic transmitter side-channel/noise problems**:

- Mixed-state MDI-QKD; Bourassa et al. Phys. Rev. A 102, 062607 (2020).
- Coherent-state MDIQKD secure against arbitrary Trojan-horse attacks; Zhang et al. PRX Quantum 2, 030304 (2021).
- Discrete phase randomization TF-QKD; Curras-Lorenzo et al. Phys. Rev. Applied 15, 014016 (2021).
- MDI-QKD with passive time-dependent source side-channels; Bourassa et al. arXiv:2108.08698 (2021); see poster # 135.

Following this body of work, alternative methods for tackling imperfect transmitter security can also be found in

- Pereira, Curty & Tamaki, npj Quantum Inf 5, 62 (2019); Pereira et al. Sci. Adv. 6, eaaz4487 (2020).
- Navarrete et al. Phys. Rev. Applied 15, 034072 (2021); see poster # 172.
- Zapatero et al. arXiv:2105.11165 (2021); see poster # 65.

Let us now consider a generic phase-encoding MDI-QKD setting whereby Eve is allowed to inject arbitrary Trojan-horse signals.

The Trojan-horse state can be written as

$$|\xi\rangle = \sum_{n,m} c_{nm} \underbrace{|n\rangle|m\rangle}_{\text{TH states}} |\mathcal{E}_{nm}\rangle, \tag{23}$$

where $|\mathcal{E}_{nm}\rangle$ is an ancilla that is kept in Eve's lab.

Let us now consider a generic phase-encoding MDI-QKD setting whereby Eve is allowed to inject arbitrary Trojan-horse signals.

The Trojan-horse state can be written as

$$|\xi\rangle = \sum_{n,m} c_{nm} \underbrace{|n\rangle|m\rangle}_{\text{TH states}} |\mathcal{E}_{nm}\rangle, \tag{23}$$

where $|\mathcal{E}_{nm}\rangle$ is an ancilla that is kept in Eve's lab.

Note that the state of the form (23) includes Trojan horses that are mixed (after tracing out Eve's ancilla) and may even be entangled.

Let us now consider a generic phase-encoding MDI-QKD setting whereby Eve is allowed to inject arbitrary Trojan-horse signals.

The Trojan-horse state can be written as

$$|\xi\rangle = \sum_{n,m} c_{nm} \underbrace{|n\rangle|m\rangle}_{\text{TH states}} |\mathcal{E}_{nm}\rangle, \tag{23}$$

where $|\mathcal{E}_{nm}\rangle$ is an ancilla that is kept in Eve's lab.

Note that the state of the form (23) includes Trojan horses that are mixed (after tracing out Eve's ancilla) and may even be entangled.

After gathering the modulation information from the modulators, the output THA state thus with the form

$$|\xi'_{xy}\rangle = \sum_{n,m} c_{nm} \underbrace{e^{i(nx+my)}}_{\text{siphoned info}} \frac{\pi}{2}|n\rangle|m\rangle|\mathcal{E}_{nm}\rangle. \tag{24}$$

Notice how the Trojan horses accumulate the phase modulation information made by Alice and Bob.

Both the quantum states prepared by Alice and Bob and the THA state will be sent to Charlie via the quantum channel.

Both the quantum states prepared by Alice and Bob and the THA state will be sent to Charlie via the quantum channel.

Like before, the untrusted measurement can be modelled by a quantum-to-classical map, which can be described by an isometry (with an appropriate purification):

$$
\begin{aligned}
|\phi_{xy}\rangle &= \underbrace{\left|e^{ix\frac{\pi}{2}}\alpha\right\rangle\left|e^{iy\frac{\pi}{2}}\beta\right\rangle}_{\text{trusted states}} \underbrace{\left|\xi'_{xy}\right\rangle}_{\text{THA states}} \\
&\to \sum_z \left|\mathrm{e}^z_{xy}\right\rangle|z\rangle.
\end{aligned} \tag{25}
$$

Then, by using the semidefinite programming, one can compute the maximum phase error rate under the assumption that the input energy of the THA states is bounded by some trusted threshold ν.

Both the quantum states prepared by Alice and Bob and the THA state will be sent to Charlie via the quantum channel.

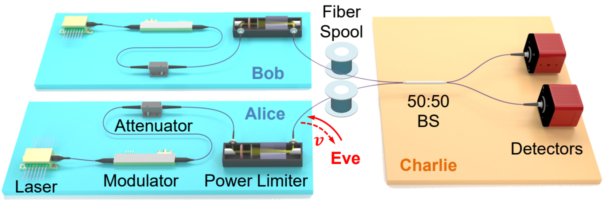
Like before, the untrusted measurement can be modelled by a quantum-to-classical map, which can be described by an isometry (with an appropriate purification):

$$|\phi_{xy}\rangle = \underbrace{\left|e^{ix\frac{\pi}{2}}\alpha\right\rangle\left|e^{iy\frac{\pi}{2}}\beta\right\rangle}_{\text{trusted states}} \underbrace{\left|\xi'_{xy}\right\rangle}_{\text{THA states}} \rightarrow \sum_z \left|\mathrm{e}^z_{xy}\right\rangle|z\rangle. \tag{25}$$

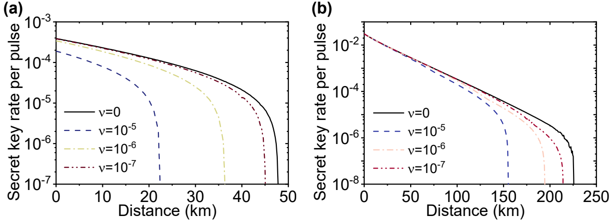
Then, by using the semidefinite programming, one can compute the maximum phase error rate under the assumption that the input energy of the THA states is bounded by some trusted threshold ν.

Experimental solutions:

- Laser induced damage threshold (LIDT); Lucamarini et al. Phys. Rev. X 5, 031030 (2015).
- Optical power limiter (passive device based on thermo-optical defocusing effects); Zhang et al. PRX Quantum 2, 030304 (2021).



(a) Phase-encoding MDI-QKD with power limiters.



(b) Left & right parameters: (a) detector's efficiency $\eta_{\text{det}} = 10\%$, dark count rate $p_{\text{dc}} = 10^{-5}$, (b) detector's efficiency $\eta_{\text{det}} = 85\%$, dark count rate $p_{\text{dc}} = 10^{-7}$. Trojan horse photon number ν of 10^{-5}, 10^{-6}, 10^{-7} and 0 are shown.

Outlook and Thank You

There are still many interesting problems:

- Numerical methods for finite-key security; see Bunandar et al. npj Quantum Inf 6, 104 (2020).

Outlook and Thank You

There are still many interesting problems:

- Numerical methods for finite-key security; see Bunandar et al. npj Quantum Inf 6, 104 (2020).
- Finite-key security of practical quantum key expansion (including authentication cost and security).

Outlook and Thank You

There are still many interesting problems:

- Numerical methods for finite-key security; see Bunandar et al. npj Quantum Inf 6, 104 (2020).
- Finite-key security of practical quantum key expansion (including authentication cost and security).
- Finite-key security of QKD with two-way classical communications.

Outlook and Thank You

There are still many interesting problems:

- Numerical methods for finite-key security; see Bunandar et al. npj Quantum Inf 6, 104 (2020).
- Finite-key security of practical quantum key expansion (including authentication cost and security).
- Finite-key security of QKD with two-way classical communications.
- Combining DV-QKD and CV-QKD; see Qi Bing's invited talk (Wed CET 4pm).

Outlook and Thank You

There are still many interesting problems:

- Numerical methods for finite-key security; see Bunandar et al. npj Quantum Inf 6, 104 (2020).
- Finite-key security of practical quantum key expansion (including authentication cost and security).
- Finite-key security of QKD with two-way classical communications.
- Combining DV-QKD and CV-QKD; see Qi Bing's invited talk (Wed CET 4pm).
- What is a good choice of security $\varepsilon_{\mathrm{qkd}}$?

Outlook and Thank You

There are still many interesting problems:

- Numerical methods for finite-key security; see Bunandar et al. npj Quantum Inf 6, 104 (2020).
- Finite-key security of practical quantum key expansion (including authentication cost and security).
- Finite-key security of QKD with two-way classical communications.
- Combining DV-QKD and CV-QKD; see Qi Bing's invited talk (Wed CET 4pm).
- What is a good choice of security $\varepsilon_{\rm qkd}$?
- And I am sure you will have some ideas as well!

Thank you! and see you in the meet-the-speaker room!